SSX0902_1 安全终端引擎

芯片白皮书

Version 2.1

北京多思科技工业园股份有限公司

http://www.t-macro.com

本文档的所有部分，其著作产权属于北京多思科技工业园股份有限公司（以下简称多思公司）所有，未经多思公司授权许可，任何个人及组织不得复制、转载、仿制本文档的全部或部分组件。本文档没有任何形式的担保、立场表达或其他暗示，若有任何因本文档或其中提及的产品所有资讯所引起的直接或间接损失，多思公司及所属员工恕不为其担保任何责任。除此以外，本文档所提到的产品规格及资讯仅供参考，内容亦会随时更新，恕不另行通知。

本文档特许以下单位作为资料参考：

- 深圳市微处理器开发研究院
- 北京南思达科技发展有限公司
- 北京天宏绎网络技术有限公司
- 北京多思科技发展有限公司

本文档所涉及的“”、“MISC”及“超弦驰”名称以及相关标识均为注册商标，其商标所有权归北京南思达科技发展有限公司所有。

本文档所涉及的可重组逻辑技术、ESOC 技术、MCOS 技术的专利权、专有技术所有权和商标权，均为北京南思达科技发展有限公司所有。

本文档所涉及的 MISC 技术的专利权、专有技术所有权，为北京多思科技工业园股份有限公司、北京南思达科技发展有限公司、北京天宏绎网络技术有限公司共同持有。

“SSX0902”是国家密码管理委员会于 2009 年 2 月为北京多思科技工业园股份有限公司的可重组体系结构密码算法芯片产品系列所授予的产品管理型号，并明确规定该产品型号已纳入国家商用密码管理。

本文档中所包含的各种算法名称仅作为标识之用，这些算法名称可能属于其他公司的注册商标或版权，在此声明。

©2009 北京多思科技工业园股份有限公司 版权所有。

北京多思科技工业园股份有限公司制作，2009 年 7 月

http:\\www.t-macro.com

目录

1. **概述** 1

1.1. 技术特点 1
1.1.1. MISC 宏指令体系结构芯片设计技术 1
1.1.2. 可重组逻辑体系结构芯片设计技术 1
1.1.3. AoC 应用在片设计技术 1
1.2. 安全特性 2
1.3. 应用特性 3
2. **芯片外特性** 4

2.1. 外部接口图 5
2.2. 信号描述 5
2.3. 时钟及电压 8
3. **接口规范** 8

3.1. 数据接口细则 9
4. **时钟设置** 10

5. **封装及管脚定义说明** 11

5.1. LQFP-100 封装 11
6. **电气特性** 15

7. **指令体系** 16

7.1. 指令功能 16
7.2. 协议指令形态 16
8. **应用指南** 19

8.1. 典型应用结构 19
8.1.1. 语音安全终端机（保密电话） 20
8.1.2. 授权设备 20
8.1.3. 刷卡设备 21

© 2009 版权所有 北京多思科技工业园股份有限公司

1. 概述

SSX0902_1 安全终端引擎芯片是针对各种类型数字终端（包括语音、数据、有线、无线终端等）的专用 AoC 安全芯片，安全功能可以实现包括密钥生成、密钥保护、证书授权、数据加解密、身份认证、数字签名、数据完整性认证等完整的安全通讯协议，保证通讯对方为合法授权用户，且通讯线路传输数据均为加密数据，其密码算法随机选择，密钥双方协商，实现一次一密及一包一密，所有安全操作均在芯片内部完成，进一步保证终端机使用的安全。

SSX0902_1 安全终端引擎芯片可应用于各种有线/无线的数字或语音终端设备，特别适合于现在发展中的电话银行、手机银行、网上证券等业务终端以及有线电话、手持终端等通讯设备，在电子商务和电子政务领域有广泛用途。

1.1. 技术特点

SSX0902_1 安全终端引擎芯片使用的主要技术包括：MISC 宏指令体系结构芯片设计技术、可重组逻辑体系结构芯片设计技术、AoC 应用在片设计技术。

1.1.1. MISC 宏指令体系结构芯片设计技术

宏指令集体系结构以算子为控制的最小成分，配合 MCOS 系统逻辑化设计，提供了可变长度的指令体系，该结构不但包含通用 CPU 具有的功能和控制，也包含专用指令和控制，使电路规模大大减小。

1.1.2. 可重组逻辑体系结构芯片设计技术

可重组逻辑体系结构设计技术使得用户可通过指令编码方式在电路逻辑上依据算法模型重组电路体系结构，重新定义数据资源和操作关系等， 根据动态编码的控制改变数据控制、操作控制、流程控制等实现不同的算法功能操作，达到最小资源集合高效支持多种算法的效果，且算法可由用户定义，可动态改变、升级。

由于该产品算法可重组改写编制，因此可以适应各国的安全保密标准，具有中性安全设计的特点，可出口。

1.1.3. AoC 应用在片设计技术

该芯片是一种软硬一体化的 AoC（应用在片）设计，采用逻辑硬化的 MCOS 系统与宏指令程序结合控制方法实现初始化控制、指令操作控制、协议控制和攻击监测、数据接口控制和其它协议连接控制。所支持的安全通讯协议及安全算法均可

© 2009 版权所有 北京多思科技工业园股份有限公司

由用户通过宏指令编码方式注入实现。

安全芯片内置 FLASH 存储器，用于保存芯片的原始设备信息、授权证书、算法编码及协议编码等。

1.2. 安全特性

SSX0902_1 安全终端引擎芯片在硬件逻辑上支持安全协议所需的操作，包括：多种公开加密对称算法、RSA 公钥算法、HASH 摘要算法、真随机数生成、素数筛选、私钥计算等。

DSL 安全通讯协议是数据链路层的安全通讯协议，由多思集团制订，国家密码管理委员会批准实施，是 SSX0902_1 安全终端引擎芯片缺省执行的安全通讯协议。DSL 协议的主要内容是：

1.采用公钥密码体制 RSA 算法实施用户密钥证书加密信息授权和证书报文加密传输；

2.采用公钥密码算法 RSA 算法与 Diffie-Hellman 密钥交换协议相结合方法，来实现身份认证、密钥协商、公共密钥计算、密钥交换；

3.采用 SHA1 摘要算法建立加密报文信息的数据认证，指令链路认证；

4.采用分组密码体制或序列密码体制实现链路数据加密处理；

5.采用孙子定理余数计算模型进行私钥（证书）存储或分储；

6.采用真随机数控制密钥生成，动态进行密码体制、密钥及存储选择；

7.采用 Lehman 算法和欧几里德算法进行素数计算和私钥计算

8.采用实时钟配置随机数与组合逻辑实现用户安全熵重组设计。

9.采用 MCOS 系统与协议结合控制方法实现算法扩展、安全监控、初始化管理。

DSL 协议实现的主要安全策略是：

- 用户公钥管理，采用 RSA 公钥密码算法，RSA 算法的大模数 n 的素因子分解的困难性和根据公钥密钥计算私钥密钥的不可能性的公钥密码特性保证了用户公钥密钥管理的安全性。
- 协议采用零知识证明的思想，保证了用户在一次交互中，用户私钥 Si，Sj 的保密性和相互可鉴别性。
- 用户公共密钥管理，采用公钥密钥加密分配用户公共密钥的方法。用户私钥 Si, Sj 的保密性，随机数 ri, rj 的随机性和不可预测性。Si, Sj 和 ri, rj 的共同作用保证了用户公共密钥分配的保密性、鉴别性和时效性。
- 用户公共密钥是由用户相互自动分配，动态改变，一次一密或一次多密的特性，保证了用户间会话通信的安全保密性。
- 用户公共密钥只是在用户一次会话时刻建立密钥，在通信之前和通信完成之后

© 2009 版权所有 北京多思科技工业园股份有限公司

均不存在密钥，密钥泄露的危险最小，不易受到攻击。

- 用户数据加密算法，使用可重组算法逻辑电路设计技术，由管理者建立算法模型，注入芯片，使用时动态安装加密算法。达到算法隐蔽的管理要求。
- 芯片内部数据读写操作均采用证书认证的安全控制方式。在可重组算法逻辑电路中由 MCOS 系统控制多个芯片之间的身份认证逻辑机制，由此可支持建立机-卡应用系统，进一步提高安全性。

1.3. 应用特性

基于 SSX0902_1 安全终端引擎芯片及其 DSL 安全通讯协议构建的 CSTU 安全终端设备具备的应用特性如下：

1. 支持授权中心通过网络授权操作：用户拨打中心管理机构的特服号，授权中心在验证用户身份后产生一个一次性用户密钥，并通过网络将授权证书注入到用户终端的安全芯片中。或授权中心以隐蔽方式主动通过网络对已授权用户终端的授权证书信息进行更改。
2. 用户申请登记授权密钥生成、一次一密保护授权信息时，采用真随机数控制密钥生成，动态进行密码体制选择；
3. 授权证书在网络上为加密传输，仅申请者可解密获取有效证书。
4. 用户证书及用户密钥加密存储；
5. 非授权用户不能进行安全通讯。
6. 采用零知识证明方式，非合法用户不能通过身份认证，具备防伪装攻击能力。
7. 采用机密信息和随机数共同计算，非经身份认证的用户不能计算出正确的公共密钥，具备抗重放攻击能力。
8. 只有拥有正确私钥的用户才能产生正确的会话密钥。
9. 所有线路传输数据均为密文，需有效密钥及算法才能正确解密获得明文。
10. 随机选择的摘要算法建立加密报文信息的数据认证，保证数据的完整性，具备防篡改攻击能力。
11. 安全策略功能。采用实时钟配置随机数与组合逻辑实现用户和系统安全熵重组设计；动态算法选择功能；一次一密功能。

可重组算法的应用特征：

1. SSX0902_1 安全终端引擎芯片支持算法重组设计，利用芯片宏指令系统和体系结构提供的算法资源 IP 模块，可以根据用户算法应用要求，设计用户自定义的算法，并加载于芯片中。详见宏指令用户手册和体系结构描述书。
2. SSX0902_1 安全终端引擎芯片还支持安全协议和安全策略的重组设计。利用芯片协议指令系统和宏指令系统用户可以设计安全协议和安全策略，并加载于芯片中。详见协议指令手册、宏指令用户手册和体系结构描述书。

© 2009 版权所有 北京多思科技工业园股份有限公司

2. 芯片外特性

本芯片在生产出厂时，仅包含公开算法的安全特性，包含 DSL 安全协议和安全策略的功能。应用中，用户可以根据需要改变算法、协议和策略的设计，并确定新的技术指标。

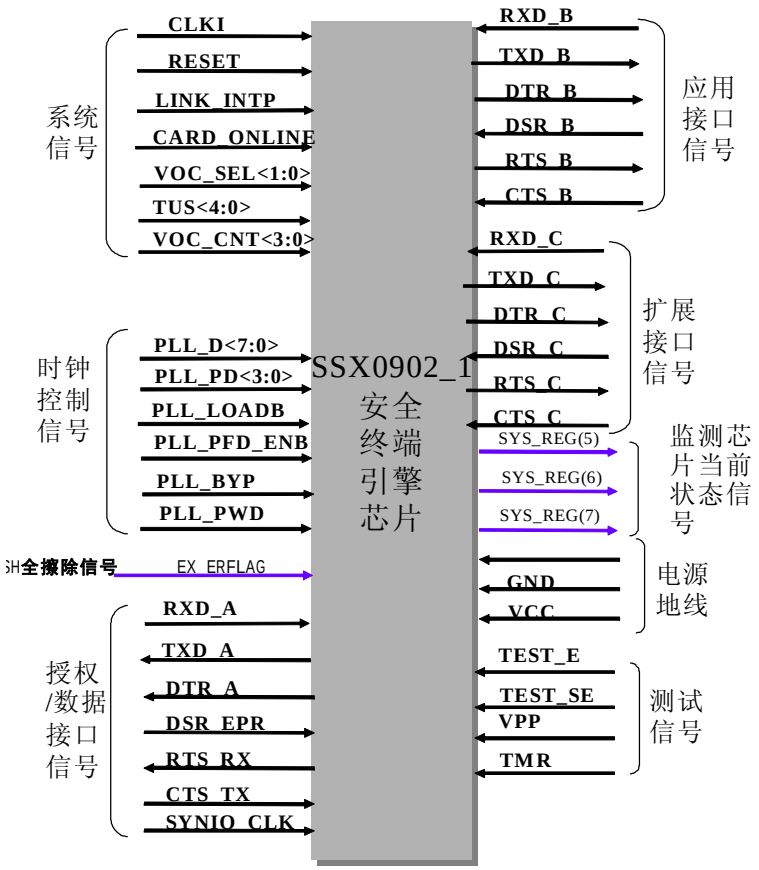
本芯片提供三个标准的 RS232 接口，可以连接语音编码器、主控 CPU、PC 机或卡证、密钥。

性能指标

- 支持标准 ECB 和 CBC 模式分组密码算法：
  - 密钥长度为 128 位的（k1,k2,k1）3DES 算法
  - 密钥长度为 128 位/192 位/256 位三种密钥长度的 RIJNDAEL 算法
- 支持标准摘要算法：
  - SHA-1 算法，160bit 摘要
- 支持用户注入使用自定义分组密码算法；
- 支持标准非对称算法：
  - 密钥长度为 1024-2048 位的 RSA 算法
  - 大素数筛选、私钥计算
  - 支持椭圆曲线 ECC 算法
- 真随机数生成

© 2009 版权所有 北京多思科技工业园股份有限公司

2.1. 外部接口图



2.2. 信号描述

PIN 名		方向	功能	备注
系统信号	CLKI	I	外部输入时钟	
	RESET	I	系统复位信号	低有效信号
	LINK_INTP	I	软复位信号	来自于应用接口连接设备，指示链路中断
	CARD_ONLINE	I	卡证在线信号	来自于扩展接口连接设备
	TUS<5:0>	I	依据设置的系统工作时钟，TUS 值为 1 微秒的系统工作时钟周期数。如当系统工作时钟设置为 20MHz 时，1 微秒为 20 周期，即 TUS 值输入为“010100”。	

© 2009 版权所有 北京多思科技工业园股份有限公司

PIN 名		方向	功能	备注
	VOC_CNT<3:0>	I	当数据接口类型选择为连接 TR600 或 AMBE2000 声码器时，该总线指明每帧数据的有效语音数据字节数	
	VOC_SEL<1:0>	I	数据接口类型选择信号。 00：RS232 接口，连接 TR600 声码器 01：主动方式同步串口，连接 AMBE2000 声码器 10：RS232 接口，连接数据源 PC 11：RS232 接口，连接授权系统 PC	依据数据接口所连接的设备类型设置。
时钟控制信号	PLL_D<7:0>	I	PLL 输出时钟的倍频调节信号，定义 M 值	PLL 输出时钟=系统输入时钟 * M/2N
	PLL_PD<3:0>	I	PLL 输出时钟的倍频调节信号，定义 N 值	PLL 输出时钟=系统输入时钟 * M/2N
	PLL_LOADB	I	PLL 模块变频控制使能信号	PLL 旁路时置“1” PLL 有效时置“0”
	PLL_PFD_ENB	I	PLL 模块控制信号，通常与 PLL_PWD 连接	旁路工作时置“1” 正常工作时置“0”
	PLL_BYP	I	PLL 模块旁路工作模式，旁路工作模式时 PLL 模块输出时钟即为输入时钟频率	旁路工作时置“1” 正常工作时置“0”
	PLL_PWD	I	PLL 模块低功耗模式，高有效	旁路模式时置“1” 正常工作时置“0”
应用接口控制信号	DSR_B	I	应用端口数据接收请求信号	低有效信号
	DTR_B	O	应用端口数据接收准备好信号	低有效信号
	CTS_B	I	应用端口数据发送许可信号	低有效信号
	RTS_B	O	应用端口数据发送请求信号	低有效信号
	SIN_B	I	应用端口数据输入线	
	SOUT_B	O	应用端口数据输出线	
扩展接口控制信号	DSR_C	I	扩展接口数据接收请求信号	低有效信号
	DTR_C	O	扩展接口数据接收准备好信号	低有效信号
	CTS_C	I	扩展接口数据发送许可信号	低有效信号
	RTS_C	O	扩展接口数据发送请求信号	低有效信号
	SIN_C	I	扩展接口数据输入线	
	SOUT_C	O	扩展接口数据输出线	
数据/授权接口控制信号	DSR_EPR	I	数据接口数据接收请求信号。 当数据接口选择为 RS232 接口时，为 DSR 数据接收请求信号；当选择为同步串口时，为 EPR 包准备好信号	当 VOC_SEL<1:0>信号线设置为 01，选择连接 AMBE2000 声码器时，与 AMBE2000 第 20 针连接；当 VOC_SEL<1:0>设置为其他值时，该信号为 RS232 接口的 DSR 信号，与对方的 RTS 信号连接
	DTR_A	O	数据接口数据接收准备好信号。	仅当连接 RS232 接口时有效，选择 AMBE2000 声码器时无效

© 2009 版权所有 北京多思科技工业园股份有限公司

PIN 名		方向	功能	备注
	CTS_TX	I	数据接口数据发送许可信号。 当数据接口选择为 RS232 接口时，为 CTS 数据发送请求信号；当选择为同步串口时，为 CHAN_TX_STRB 输出使能信号	当 VOC_SEL<1:0>信号线设置为 01，选择连接 AMBE2000 声码器时，与 AMBE2000 第 38 针连接；当 VOC_SEL<1:0>设置为其他值时，该信号为 RS232 接口的 CTS 信号，与对方的 DTR 信号连接
	RTS_RX	O	数据接口数据发送请求信号。 当数据接口选择为 RS232 接口时，为 RTS 数据发送准备好信号；当选择为同步串口时，为 CHAN_RX_STRB 输入使能信号	当 VOC_SEL<1:0>信号线设置为 01，选择连接 AMBE2000 声码器时，与 AMBE2000 第 30 针连接；当 VOC_SEL<1:0>设置为其他值时，该信号为 RS232 接口的 RTS 信号，与对方的 DSR 信号连接
	RXD_A	I	授权/数据接口数据输入线	当 VOC_SEL<1:0>信号线设置为 01，选择连接 AMBE2000 声码器时，与 AMBE2000 第 42 针连接；当 VOC_SEL<1:0>设置为其他值时，该信号为 RS232 接口的 RXD 信号，与对方的 TXD 信号连接
	TXD_A	O	授权/数据接口数据输出线	当 VOC_SEL<1:0>信号线设置为 01，选择连接 AMBE2000 声码器时，与 AMBE2000 第 32 针连接；当 VOC_SEL<1:0>设置为其他值时，该信号为 RS232 接口的 TXD 信号，与对方的 RXD 信号连接
	SYNIO_CLK	O	数据接口采集时钟	为系统工作时钟的一致。VOC_SEL<1:0>信号线设置为 01，选择连接 AMBE2000 声码器时，与第 28 和第 34 针连接
测试信号	TEST_E	I	芯片测试模式	正常工作时置“0”
	TEST_SE	I	芯片扫描链使能模式	正常工作时置“0”
	VPP	I	FLASH 测试信号	正常工作时悬空
	TMR	I	FLASH 测试信号	正常工作时置“1”
状态位	STS_REG5	O	监测芯片当前状态信号	初值为“0”
	STS_REG6	O	监测芯片当前状态信号	初值为“0”
	STS_REG7	O	监测芯片当前状态信号	初值为“0”
FALSH 擦除	EX_ERFLAG	I	芯片测试时外部的 FLASH 全擦信号	高电平有效
电源 PIN	GND			
	VCC			

© 2009 版权所有 北京多思科技工业园股份有限公司

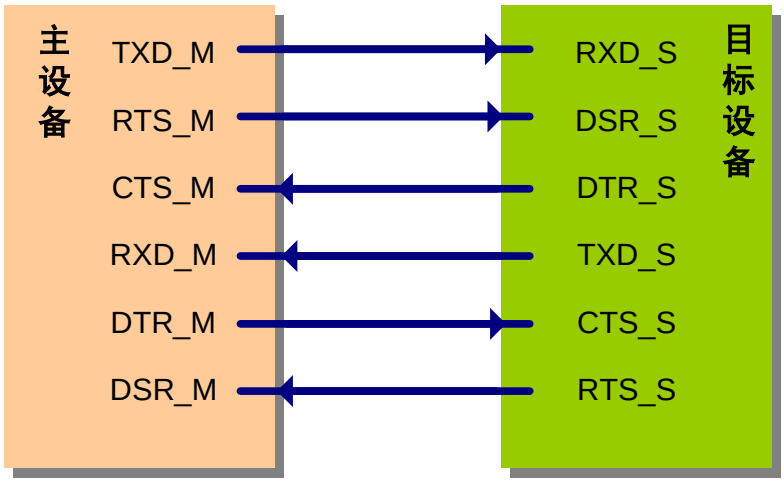
2.3. 时钟及电压

- 工作电压为 3.3V，核心电路为 2.5V；可适应 5%电压浮动范围
- 外部输入时钟频率范围：2MHz~20MHz
- 芯片制造工艺：0.25u
- 封装方式：LQFP_80 Pin、LQFP_100 Pin
- 功耗：<0.4W

3. 接口规范

SSX0902_1 安全终端引擎芯片具有三个标准的 RS232 接口。

RS232 内核由 MCOS 程序控制，MCOS 内核实现对 RS232 的接口标准协议的管理，完成标准 RS232 接口的数据交换。



信号关系连接图

接口 A：用户语音终端时连接语音编解码芯片，授权设备时连接授权中心管理系统 PC；称为数据接口或授权接口。注意：接口 A 连接语音编解码芯片时，可以配置为同步串口通讯方式。详见 3.1 节数据接口细则

用户安全设备连接语音或数据，实现语音或数据加密通讯；授权安全设备连接控制管理系统主机（PC），实现证书颁发、更新，用户信息管理；

接口 B：与安全设备的主控芯片连接，称为应用接口。

CSTU 安全终端的主控芯片管理键盘、液晶显示、网络通讯等设备，具备普通数字终端的应用功能。

© 2009 版权所有 北京多思科技工业园股份有限公司

CSTU 安全终端在连接网络的设计是统一和一致的：通过设备的 MCU 管理实现 PSTN、ETHERNET、DDN、ISDN、ADSL 等网络通讯、数据传输。

接口 C：可连接 CPU 卡或密钥，称为扩展接口。

扩展连接的卡或密钥可用于实现证书、算法、协议、密钥扩展。

接口 A 是必须的，但其连接关系因设备类型不同连接关系有所不同：用户设备时连接语音或数据源；授权设备时连接授权管理系统；在某些特定应用中，如银行系统的键盘加密板，需加密传输的数据源直接由终端设备的主控芯片采集键盘输入时，接口 A 可不用。
接口 B 是必须的，仅与安全终端的主控 MCU 连接；

接口 C 是可选的。

3.1. 数据接口细则

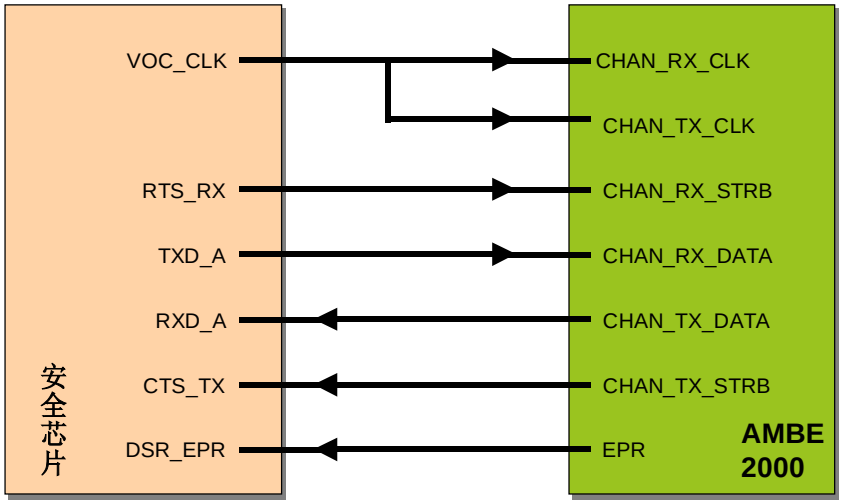
SSX0902_1 安全终端引擎芯片提供接口 A 用于连接管理系统主机或语音编解码芯片或其他数据源。连接管理系统主机时接口规范为 RS232；连接语音编解码芯片时可选择连接 AMBE2000 声码器或 TR600 声码器，安全芯片可自适应是识别 AMBE2000 或 TR600 的帧数据格式；或者可以连接 PC 做为加密传输的数据源。

芯片管脚 VOC_SEL<1:0>用于选择接口 A 所连接的设备类型。

VOC_SEL<1>	VOC_SEL<0>	接口设置
0	0	连接 TR600 声码器，接口规范为 RS232 接口；支持 600/800/1200/2400bps 的编码率
0	1	连接 AMBE2000 声码器，接口规范为同步串口。此时 AMBE2000 声码器的接口设置为主动模式帧传输方式（CH_SEL<1:0>设置为“00”；支持 2000 或 2400bps 的编码率
1	0	连接 PC，接口规范为 RS232 接口
1	1	保留

当 VOC_SEL<1:0>设置为“01”，连接 AMBE2000 声码器时，CSTU 安全终端引擎芯片和 AMBE2000 声码器的连接关系如下：

© 2009 版权所有 北京多思科技工业园股份有限公司



连接 AMBE-2000 声码器芯片时，除串行接口连接如上图所示外，AMBE-2000 声码器芯片的其他管脚应该做如下设定：

AMBE2000管脚信号	设定值	说明
CH_SEL<1:0>	“00”	应用接口的串行接口为被动模式，格式化的帧输入输出
RATE_SEL<4:0>	“00000”	编码率 2400bps，全部为语音数据
	“00101”	编码率 2400bps，其中语音数据为 2350bps，FEC 纠错码 50bps
	“11111”	编码率 2000bps，全部为语音数据

4. 时钟设置

SSX0902_1 安全终端引擎芯片系统工作时钟为 20MHz（大约）。系统工作时钟可以直接为系统输入时钟，也可以使用芯片内 PLL 模块输出时钟。

当系统输入时钟约为 80MHz 时，置 PLL_BYP 管脚信号为“1”，则片内 PLL 呈旁路模式，系统输入时钟即为 PLL 模块输出时钟；

当电路板上提供的系统输入时钟不足 10MHz 时，置 PLL_BYP 管脚信号为“0”，则片内 PLL 呈工作模式，PLL 模块输出时钟即为系统工作时钟。

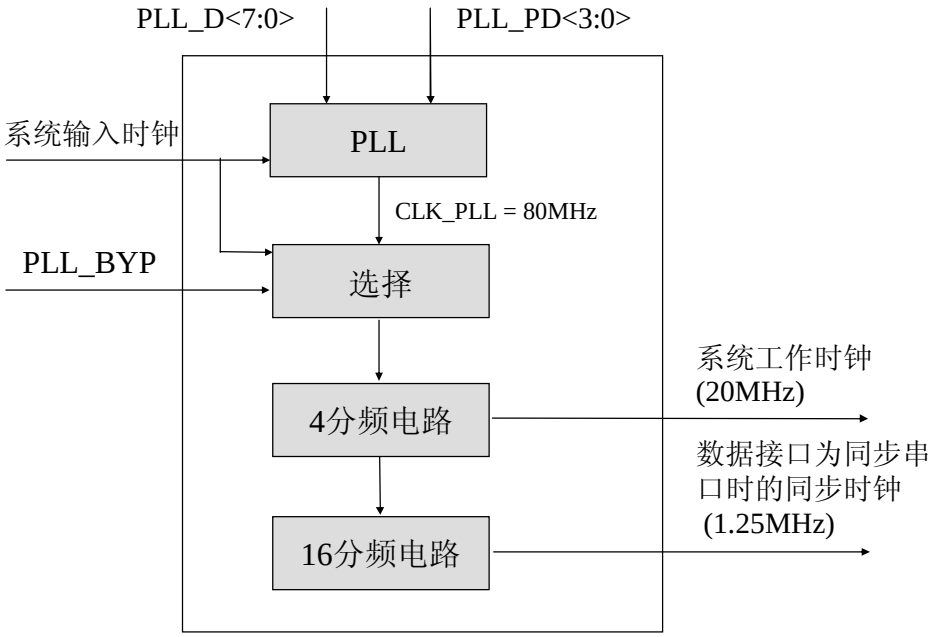
PLL 模块的输出频率根据系统输入时钟，通过 PLL_D<7:0>端口及 PLL_PD<3:0>的设置，在高于 3.125MHz、低于 250MHz 范围内可调，PLL 输出频率计算公式如下：

PLL 输出频率 = 输入频率 * M / 2N
其中：PLL_D 值标为 M（M≥2），PLL_PD 值标为 N（N≥1），输入频率不低于 2MHz。

© 2009 版权所有 北京多思科技工业园股份有限公司

当数据接口连接为 AMBE2000 声码编解码芯片时，数据接口采用同步串行接口规范，其中接口同步时钟为系统工作时钟的 16 分频。

如下图所示：



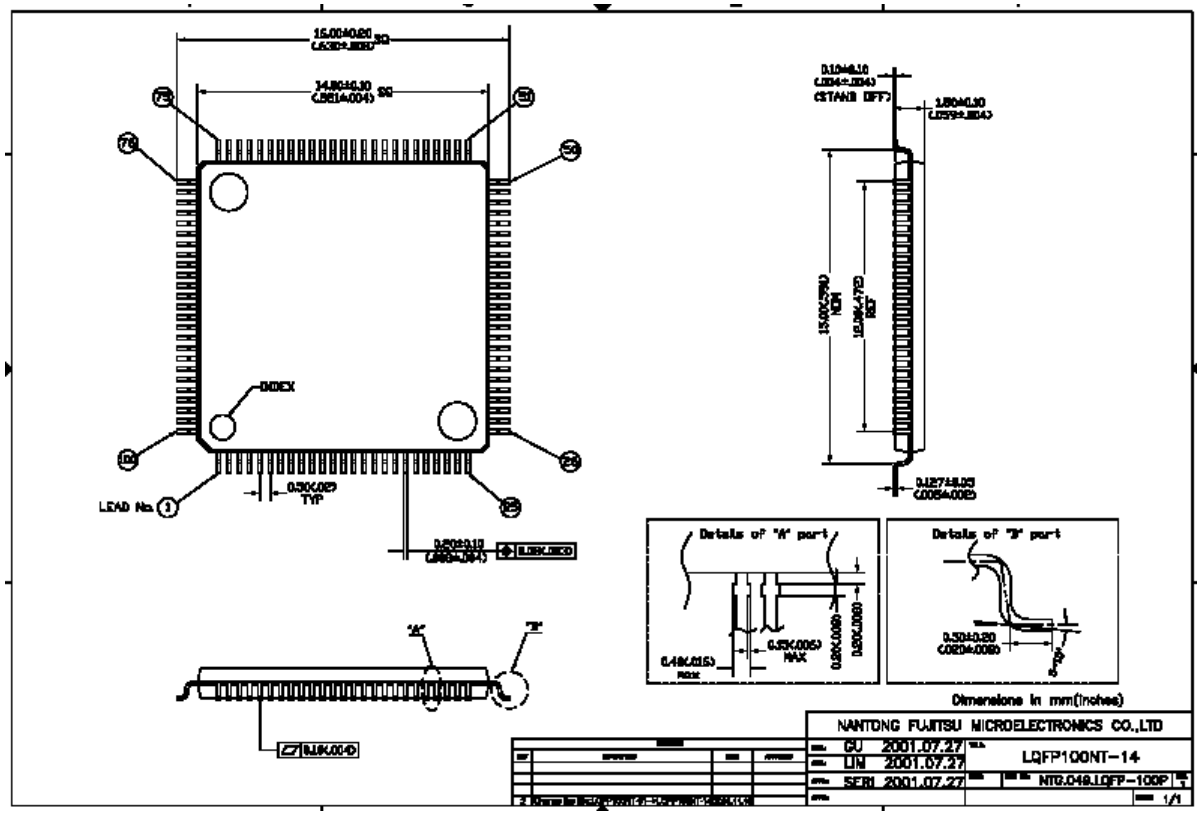
例：当系统输入时钟为 5MHz 时，置 PLL_BYP 为“0”，将 PLL_D<7:0>设为“00001000”（M=8），PLL_PD<3:0>设为“0001”（N=1），PLL 输出时钟为 5MHz * 8/2 = 20MHz，为系统工作时钟。数据接口为同步串口时的同步时钟为 20/16 = 1.25MHz。

5. 封装及管脚定义说明

SSX0902_1 安全终端引擎芯片的封装方式为 100 pinLQFP 封装。其中 100 pin 的 LQFP 封装有效 I/O 信号管脚 55 条，测试管脚 5 条，电源地管脚 28 条,置空管脚 12 条。

5.1. LQFP-100 封装

© 2009 版权所有 北京多思科技工业园股份有限公司



PIN 号	PIN 名	方向	功能
1	VOC_SEL[0]	I	VOC_SEL[1：0]指明数据接口类型选择信号。 00：RS232 接口，连接 TR600 声码器 01：主动方式同步串口，连接 AMBE2000 声码器 10：RS232 接口，连接数据源 PC 11：RS232 接口，连接授权系统 PC
2	VOC_SEL[1]	I	
3	VOC_CNT[0]	I	VOC_CNT[3：0]当数据接口类型选择为连接 TR600 或 AMBE2000 声码器时，该总线指明每帧数据的有效语音数据字节数
4	FLTEST_MODE	I	片内 FLASH 的测试模式信号。正常工作状态下置‘0’
5	VOC_CNT[1]	I	
6	VOC_CNT[2]	I	
7	VOC_CNT[3]	I	
8	vdd1	Power	2．5V 核心供电电源
9	vdd1		
10		NC	
11	gnd1	Ground	核心供电地
12	gnd1	Ground	核心供电地
13	TEST_SE	I	测试模式下扫描链使能信号，正常工作状态接 0
14	TEST_E	I	测试模式时接 1，正常工作状态接 0
15	RESET	I	系统复位信号，低电平有效
16	vdd2	Power	3．3V 数字 IO 电源
17	SYNIO_CLK	O	数据接口采集时钟

© 2009 版权所有 北京多思科技工业园股份有限公司

PIN 号	PIN 名	方向	功能
18	gnd2	Ground	数字 IO 地
19	STS_REG5	O	监测芯片当前状态信号　　初值为“0”
20	DTR_A	O	数据接口数据接收准备好信号。
21	RTS_RX	O	数据接口数据发送请求信号。 当数据接口选择为 RS232 接口时，为 RTS 数据发送准备好信号；当选择为同步串口时，为 CHAN_RX_STRB 输入使能信号。
22	TXD_A	O	授权/数据接口数据输出线
23	CTS_TX	I	数据接口数据发送许可信号。 当数据接口选择为 RS232 接口时，为 CTS 数据发送请求信号；当选择为同步串口时，为 CHAN_TX_STRB 输出使能信号。
24	DSR_EPR	I	数据接口数据接收请求信号。 当数据接口选择为 RS232 接口时，为 DSR 数据接收请求信号；当选择为同步串口时，为 EPR 包准备好信号
25	RXD_A	I	授权/数据接口数据输入线
26	gnd1	Ground	核心供电地
27		NC	
28	vdd1	Power	2．5V 核心供电电源
29	PLL_D[7]	I	PLL 输出时钟的倍频调节信号，详见 4 节“时钟设置”说明
30	PLL_D[6]	I	PLL 输出时钟的倍频调节信号，详见 4 节“时钟设置”说明
31	PLL_D[5]	I	PLL 输出时钟的倍频调节信号，详见 4 节“时钟设置”说明
32	PLL_D[4]	I	PLL 输出时钟的倍频调节信号，详见 4 节“时钟设置”说明
33	STS_REG6	O	监测芯片当前状态信号　　初值为“0”
34	PLL_D[3]	I	PLL 输出时钟的倍频调节信号，详见 4 节“时钟设置”说明
35	PLL_D[2]	I	PLL 输出时钟的倍频调节信号，详见 4 节“时钟设置”说明
36	PLL_D[1]	I	PLL 输出时钟的倍频调节信号，详见 4 节“时钟设置”说明
37	PLL_D[0]	I	PLL 输出时钟的倍频调节信号，详见 4 节“时钟设置”说明
38	PLL_BYP	I	PLL 模块旁路工作模式，为 1 时 PLL 模块输出时钟即为输入时钟频率，正常工作时置“0”
39	STS_REG7	O	监测芯片当前状态信号　　初值为“0”
40	PLL_PD[0]	I	PLL 输出时钟的倍频调节信号，详见 4 节“时钟设置”说明
41	PLL_PD[1]	I	PLL 输出时钟的倍频调节信号，详见 4 节“时钟设置”说明
42	PLL_PD[2]	I	PLL 输出时钟的倍频调节信号，详见 4 节“时钟设置”说明
43	PLL_PD[3]	I	PLL 输出时钟的倍频调节信号，详见 4 节“时钟设置”说明
44	gnda1	Analog ground	与 pin47 连接，不能和其他 Ground 连接
45	vdda1	Analog power	与 pin48 连接，不能和其他 Power 连接
46		NC	
47	gnda1	Analog ground	
48	vdda1	Analog power	
49		NC	
50	gnda2	Analog ground	模拟 IO 地
51		NC	

© 2009 版权所有 北京多思科技工业园股份有限公司

PIN 号	PIN 名	方向	功能
52	gnda1	Analog Ground	3．3V 电源保护环 Ground
53		NC	
54	vdda1	Analog Power	3．3V 电源保护环 Power
55	vdda2	Power	3．3V 模拟 IO 电源
56	CLKI	I	系统时钟输入
57	gnd1	Ground	核心供电地
58	PLL_PFD_ENB	I	PLL 模块控制信号，通常与 PLL_PWD 连接，正常工作时置“0”
59	PLL_PWD	I	PLL 模块低功耗模式，高有效。正常工作时置“0”
60		NC	
61	PLL_LOADB	I	PLL 模块变频控制使能信号，正常工作时置“1”
62	vdd1	Power	3．3V 核心供电电源
63	CARD_ONLINE	I	扩展接口连接设备在线指示，高电平有效
64	EX_ERFLAG	I	芯片测试时外部的 FLASH 全擦信号　高电平有效
65	SIN_C	I	扩展接口数据输入线
66	DSR_C	I	扩展接口数据接收请求信号
67	CTS_C	I	扩展接口数据发送许可信号
68	SOUT_C	O	扩展接口数据输出线
69		NC	
70	RTS_C	O	扩展接口数据发送请求信号
71	DTR_C	O	扩展接口数据接收准备好信号
72	vdd2	Power	3．3V 数字 IO 电源
73	gnd2	Ground	数字 IO 地
74	vdd2	Power	3．3V 数字 IO 电源
75	gnd2	Ground	数字 IO 地
76	TUS[0]	I	依据设置的系统工作时钟，TUS<5:0>值为 1 微秒的系统工作时钟周期数。
77	gnd1	Ground	核心供电地
78		NC	
79	gnd1		
80	TUS[1]	I	
81	TUS[2]	I	
82	TUS[3]	I	
83	TUS[5]	I	
84	TUS[4]	I	
85	TMR	I	Flash 测试信号。正常使用时，接 VDD
86	vdd1	Power	2．5V 核心供电电源
87		NC	
88	vdd1	Power	2．5V 核心供电电源
89	VPP	I	Flash 测试信号。正常使用时悬空

© 2009 版权所有 北京多思科技工业园股份有限公司

PIN 号	PIN 名	方向	功能
90	gnd2	Gruond	数字 IO 地
91	SOUT_B	O	应用接口数据输出线
92		NC	
93	RTS_B	O	应用接口数据发送请求信号
94	vdd2	Power	3．3V 数字 IO 电源
95	DTR_B	O	应用接口数据接收准备好信号
96	CTS_B	I	应用接口数据发送许可信号
97	DSR_B	I	应用接口数据接收请求信号
98	SIN_B	I	应用接口数据输入线
99		NC	
100	LINK_INTP	I	软复位信号，高电平有效。用于应用接口指明通讯链路中断

6. 电气特性

标准使用环境

参数		最小值	正常值	最大值	单位
DV_{DD}	I/O Supply Voltage	3	3.3	3.6	V
V_{SS}	Supply Voltage	-	0	-	V
V_{IH}	High-level input voltage	2	-	DV_{DD} + 0.3	V
V_T	Threshold point	1.24	1.38	1.58	V
V_{IL}	Low-level input voltage	-0.3	-	0.8	V
I_{OH}	High-level output current	* 3.0[1]	6.2	10.0	**mA**
		# 5.7[2]	11.6	18.6	**mA**
I_{OL}	Low-level output current	* 2.0	3.3	4.1	**mA**
		# 4.1	6.7	8.2	**mA**

在标准温度环境下的电器特性

参数		测试条件	MIN	TYP	MAX	单位
V_{OH}	High-level output voltage‡	V_{DD} = 3.3 ±V, I_{OH} = MAX	2.4			V
V_{OL}	Low-level output voltage‡	I_{OL} = MAX			0.4	V
I_I	Input current in high impedance ($V_I = V_{SS}$ to V_{DD})	V_{DD} = MAX, $V_I = V_{SS}$ to V_{DD}	-10		10	**μA**
C_I	Input capacitance			10		**pF**
C_O	Output capacitance			15	30	**pF**

1 * 为管脚列表中输出驱动电流为2mA的输出管脚电流值。

2 # 为管脚列表中输出驱动电流为 4mA 的输出管脚电流值。

© 2009 版权所有 北京多思科技工业园股份有限公司

7. 指令体系

CSTU 安全终端应用指令是授权中心管理软件、安全设备主控芯片应用系统软件与 CSTU 安全芯片、及 CSTU 安全芯片与 CSTU 安全芯片之间通讯的应用层指令，是实施基于 SSX0902_1 安全终端引擎芯片、实现安全通讯以及安全管理的应用系统开发的指令体系。

7.1. 指令功能

SSX0902_1 安全终端引擎芯片应用指令体系从指令功能上划分包括：

1. 注入指令：实现芯片原始信息、算法编码、协议编码的注入加载。
2. 接口应答指令：安全芯片与三个接口所连接（芯片）设备之间传输的反映接口操作状态或设备状态的指令。
3. 接口初始化指令：从安全芯片三个任意接口接到初始化指令，可以对三个任意接口的波特率进行设置。
4. 接口传输指令：由 SSX0902_1 安全终端引擎芯片与三个接口所连接（芯片）设备之间交换数据的指令。
5. 操作指令：由安全芯片三个接口的应用端向安全芯片发出的安全操作指令，反映用户的安全操作需求，该类操作指令通常是安全终端设备使用时对安全芯片的启动指令。
6. 通讯指令：由两个 CSTU 安全终端之间通过网络传输给对方的通讯指令。包括：密钥交换、密钥协商、摘要传输指令、密文数据传输指令、数字签名数据传输指令。
7. 宏指令：执行应用程序设计的指令集

7.2. 协议指令形态

SSX0902_1 安全终端引擎芯片应用指令集的协议指令形态以 8 位为基本形态，部分指令为 16 位指令形态；仅数据区注入指令为 24 位指令形态。

15	14	13	12	11	10	9	8
00 主功能 1		00 子功能 1		00 接口交互指令		00 空操作	
						01 读设备初始化信息	
						10 读时钟	
						11 操作结束	

15	14	13	12	11	10	9	8
00 主功能 1		00 子功能 1		01 输入指令		00 包错误	
						01 使用用户定义熵通讯	
						10 起动程序 1	
						11 起动程序 2	

© 2009 版权所有 北京多思科技工业园股份有限公司

15	14	13	12	11	10	9	8
00 主功能 1		00 子功能 1		10 显示指令 1		00 白裸片	
						01 第二机关白裸片	
						10 第三机关白裸片	
						11 授权未完成	
				11 显示指令 2		00 初始化完毕	
						01 安全链路建立完毕	
						10 授权失败	
						11 授权成功	
00 主功能 1		01 子功能 2		00 操作状态 1		00 许可通讯	
						01 同网错误	
						10 卡不在线	
						11 声码器不在线	
		01 子功能 2		01 操作状态 2		00 操作错误	
						01 操作正确	
						10 无法授权	
						11 无法通讯	
		01 子功能 2		10 操作状态 3		00 身份错误	
						01 设备状态错误	
						10 授权许可	
						11 证书过期	

15	14	13	12	11	10	9	8
00 主功能 1		01 子功能 2		11 应答指令		00 扩展加密	
						01 扩展解密	
						10 时钟错误	
						11 返回时钟	
00 主功能 1		10 子功能 3		00 接口初始化		接口选择	
						00：RS232A	
						01：RS232B	
						10：RS232C	
						11:保留	
				01 返回初始化信息		数据长度	
				1 加密通讯	（授权机时）电话号码长度		
						协议选择	主叫/被叫

15	14	13	12	11	10	9	8
00 主功能 1		11 子功能 4		00 键值操作指令		00 64 位键值数据解密	
						01 128 位键值数据解密	
						10 64 位键值数据明文输出	
						11 128 位键值数据明文输出	
00 主功能 1		11 子功能 4		01 语音数据输出指令		00 64 位解密语音数据输出	
						01 128 位解密语音数据输出	
						10 64 位加密语音数据输出	
						11 128 位加密语音数据输出	
00 主功能 1		11 子功能 4		10 语音数据处理指令		00 64 位语音数据处理	
						01 128 位语音数据处理	
						10 保留	
						11 保留	
00 主功能 1		11 子功能 4		11 启动指令 3			

15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
01 主功能 2		00 子功能 1		00 协议数据输出		数据长度									
				01 密钥协商		数据长度									

© 2009 版权所有 北京多思科技工业园股份有限公司

15 14	13 12	11 10	9 8	7 6	5 4	3 2	1 0
		10 申请验证登记	数据长度				
		11 身份认证	数据长度				
01 主功能 2	01 子功能 2	00 签发用户证书	数据长度				
		01 签发解析证书	数据长度				
		10 签发签权证书	数据长度				
×		11 启动指令 4					

15 14	13 12	11 10	9 8	7 6	5 4 3 2 1 0
01 主功能 2	10 子功能 3	00 读密钥	密钥类型选择	密钥数据选择	数据长度
		01 返回密钥	密钥类型选择	密钥数据选择	数据长度
		10 密钥分储	密钥类型选择	密钥数据选择	数据长度
		11 密钥交换	类型选择	密钥数据选择	数据长度

15 14	13 12	11 10	9 8	7 6 5 4 3 2 1 0
01 主功能 2	11 子功能 4	00 用户输入	00 口令	数据长度，8 位数据位一个计数长度
			01 加密算法	数据长度，8 位数据位一个计数长度
			10 摘要算法	数据长度，8 位数据位一个计数长度
			11 密钥策略	数据长度，8 位数据位一个计数长度
		01 管理输入	0 0 口令	数据长度，8 位数据位一个计数长度
			01 用户安全熵	数据长度，8 位数据位一个计数长度
			10 系统安全熵	数据长度，8 位数据位一个计数长度
			11 密钥策略	数据长度，8 位数据位一个计数长度

15 14	13 12	11 10	9 8	7 6 5 4 3 2 1 0
01 主功能 2	11 子功能 4	10 接口指令	00 返回授权参数	数据长度，8 位数据位一个计数长度
			01 起动指令 5	
			10 起动指令 6	
			11 起动指令 7	
01 主功能 2	11 子功能 4	11 传输指令	00 摘要数据传输指令	数据长度，8 位数据位一个计数长度
			01 密文数据传输指令	
			10 数字签名传输指令	
			11 初始化信息传输指令	

15 14	13 12	11 10	9 8 7 6 5 4 3 2 1 0
10 主功能 3	00 子功能 1	00 信息区注入	

© 2009 版权所有 北京多思科技工业园股份有限公司

15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
				01 数据区注入		（注：24 位指令形态）									
				10 读签权证书指令		签权证书长度									
				11 返回签权证书		签权证书长度									

15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
10 主功能 1		01 子功能 2		00 更新授权		授权机关选择		证书编号			协议选择	类型（用户密钥证书或签权证书）	保留，用户电话号码长度		
				01 申请授权		授权机关选择		证书编号			协议选择	首次或更改	保留		
				10 读授权机关参数		授权机关选择		证书编号			保留	保留	参数选择		
				11 授权更新注入		授权机关选择		证书编号			协议选择	类型（信息区或主存区）	保留，用户电话号码长度		

15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
10 主功能 3		10 子功能 3		00 数据加密指令 01 数据解密指令 10 返回加密数据指令 11 返回解密数据指令		保留 保留 分组选择 保留	数据长度								
		11 起动指令 8													

协议指令应用规范详见《CSTU 安全终端机协议应用指令手册》

宏指令应用规范详见《CSTU 安全终端机宏应用指令手册》

8. 应用指南

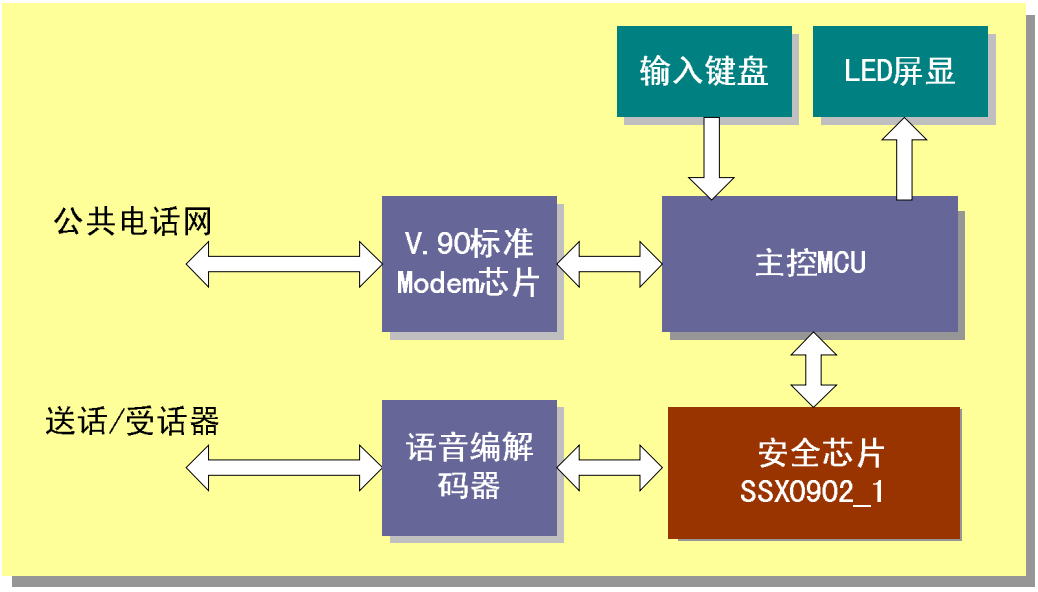
8.1. 典型应用结构

CSTU 安全终端机的应用设计范畴包括：语音、图象、数据加密，可以应用于加密机产品设计、保密电话机产品设计、单兵短波加密步话机设计、安全电话银行（证卷）系统、交易系统等产品的应用设计。

© 2009 版权所有 北京多思科技工业园股份有限公司

8.1.1. 语音安全终端机（保密电话）

有线语音安全终端机（保密电话）由 SSX0902_1 安全终端引擎芯片、语音编解码器、PCM、MODEM 等其他辅助处理器芯片、电话主控芯片 MCU 以及配属的连接设备（PSTN 及可以连接计算机的 USB/RS232 端口）构成完整系统。



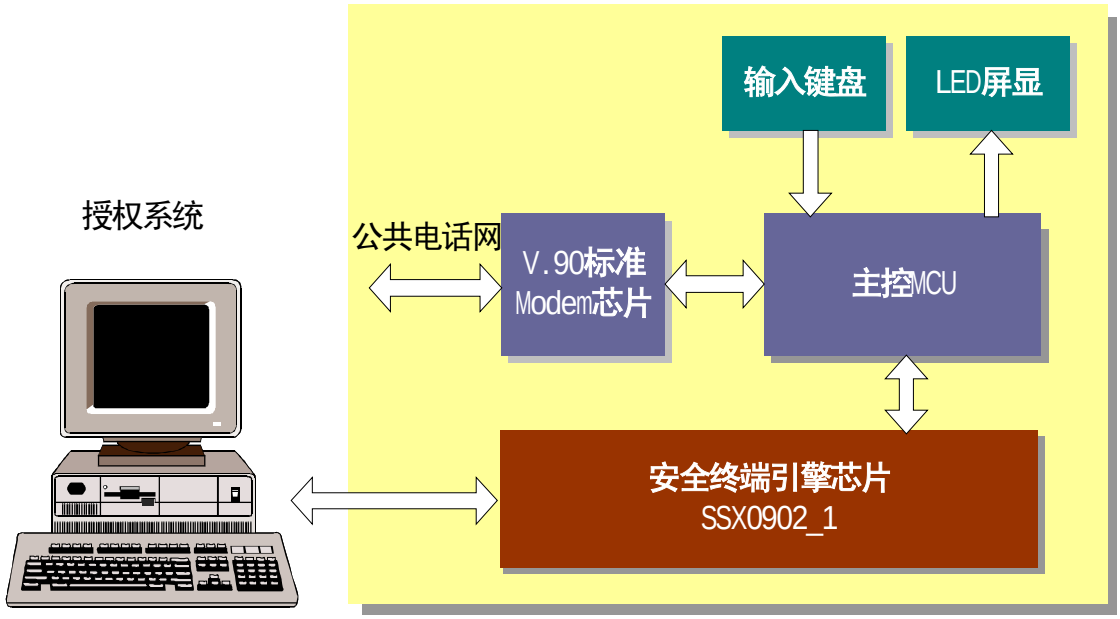
电话主控芯片 MCU 功能包括：

1. 电话通讯链路建立
2. 用户面板键盘控制
3. LCD 显示控制
4. MODEM 调制解调控制

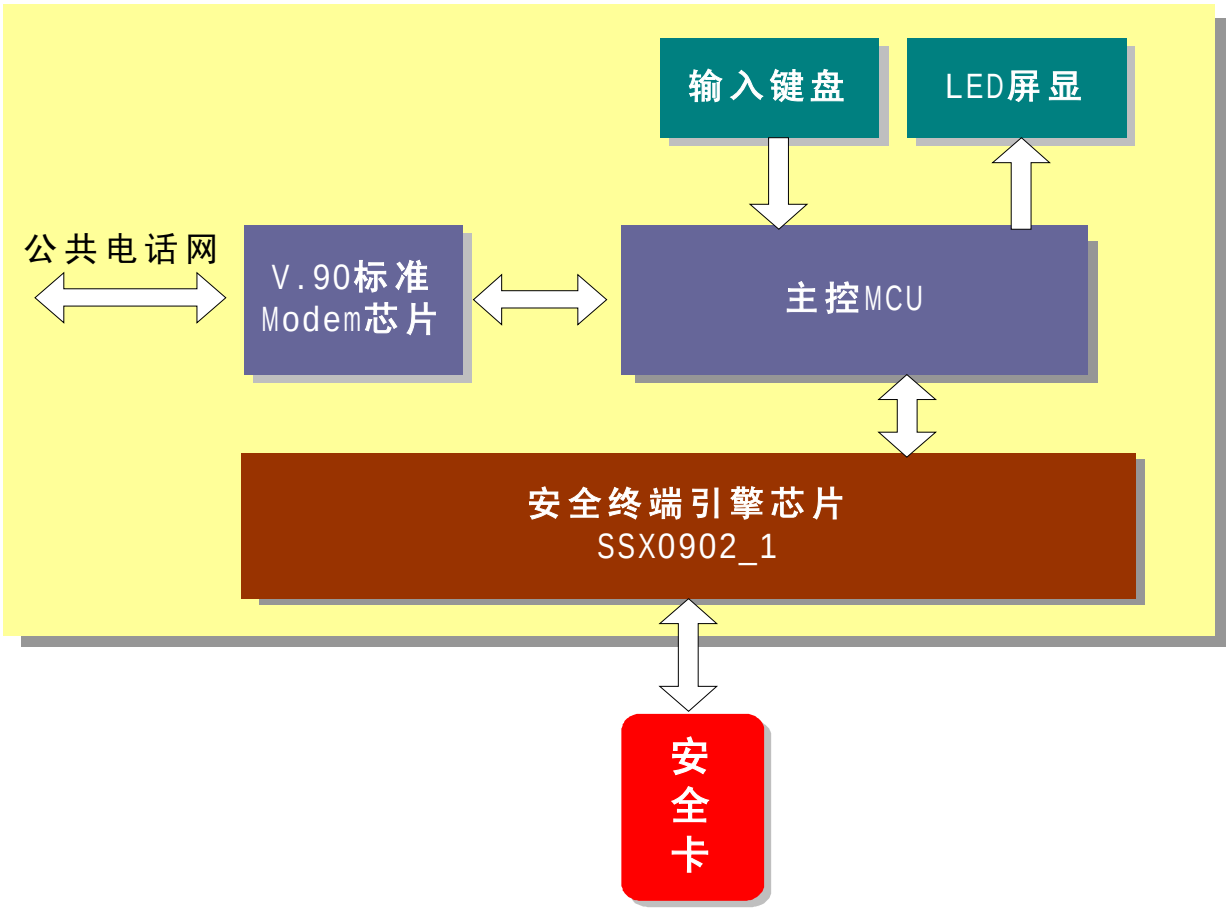
8.1.2. 授权设备

配合 CSTU 安全终端用户机使用的授权设备在授权服务中心使用，负责用户机的证书授权、信息管理等。授权设备挂接在授权系统服务器上，通过授权接口与授权系统连接。

© 2009 版权所有 北京多思科技工业园股份有限公司



8.1.3. 刷卡设备



© 2009 版权所有 北京多思科技工业园股份有限公司